FRAUD

402 reported in 2001 · 490 reported in 2002

The FBI's Uniform Crime Reporting System does not include fraud, false pretenses, forgery, embezzlement, and confidence games among larceny. Yet in many cases, fraud is a much more serious crime than theft. Victims of check forgery and "con" games stand to lose thousands of dollars. Often added to this loss is the personal humiliation that accompanies being "duped" by a "con man." The confidence game crook, a particularly crafty breed of criminal who has no qualms with deceiving his victims face-to-face, expects that his victim's embarrassment will deter him or her from reporting the crime to the police.

In 2002, 490 incidents of fraud and forgery were reported to the Cambridge Police, ranging from simple check forgery to elaborate confidence swindles. Even though this may seem like an alarming number, this crime is thought to be substantially underreported. The following defines the categorizations that the Crime Analysis Unit uses when differentiating these fraudulent episodes, as well as a few highlights of this past year's activity throughout the city:

Crime	2001	2002
Counterfeiting	**9**	**2**
Forgery/Uttering	**254**	**332**
Application	0	2
Bad Check	17	36
Forged Check	72	72
Credit/ATM Card	165	212
Other/Misc.	0	10
Con Games	**22**	**37**
Big Carrot	5	8
Utility Impostor	4	2
Pigeon Drop	1	9
Charity Impostor	1	6
Psychic Swindle	1	0
Travel Scam	0	1
Odd Jobs	1	0
Internet Related	0	2
Miscellaneous	9	9
Embezzlement	**17**	**5**
Identity Theft	**83**	**115**

CHECK FORGERY (72 incidents): This type of forgery is quite self-explanatory – someone manages to obtain checks that are not his/hers, forges their signature to look like that of the rightful owner, and cashes the check in exchange for cash, or possibly to purchase merchandise. Forgers manage to acquire some of the victim's checks generally through purse theft or by intercepting them in the mail. Often, the victim does not learn of the theft until he or she receives his or her next balance statement—by this time, the thief may have depleted the account of thousands of dollars. The number of reported incidents in 2002 remained the same as in 2001, with a total of 72 incidents. It is most likely that this category of fraud is one of the most underreported type, typically due to the fact that the victim feels that nothing can be done about the situation.

CREDIT CARD/ATM CARD FRAUD (212 incidents): Another simple scenario: a thief steals a credit card or ATM card (or copies the card number) from his victim, then uses it to purchase expensive items or deplete the owner's account. Again, the victim sometimes does not discover the theft until he or she receives a balance statement. There were 124 reported cases of credit card/ATM fraud in 1997, and it has since doubled to 212 in 2002.

APPLICATIONS (2 incidents): Forgery of applications occurs when a suspect goes into a commercial establishment and applies for a store credit card. After the application is falsely filed out, the suspect charges merchandise on the credit card and then never pays the balance. In 2000, eight incidents were reported, zero in 2001, and two in 2002. The first incident transpired in June when a young man signed his father's name to a student loan in the amount of nearly $15,000. The second incident occurred in August when a woman was contacted by her credit card company that an unknown person used the victim's information to open a credit card account via mail and was denied.

COUNTERFEITING (2 incidents): Counterfeiting is one of the more devious types of fraud. True counterfeiters invest thousands of dollars for counterfeiting equipment to produce near copies of genuine dollar bills. Because of the cost, counterfeited bills are usually of high denomination. The two incidents this year in Cambridge involved $20 and $100 bills. The first incident occurred in late July when two men from Connecticut were arrested after they passed counterfeit $100 bills at a restaurant in the Highlands section of the city. A total of three $100 bills were found on their person along with two $20 bills, and an additional three $100 bills were found at the restaurant. The second

incident occurred at the Galleria when two suspects passed a false $100 bill for a $50 purchase. It is very likely that there were more bills passed in 2002 that went undetected.

EMBEZZLEMENT (5 incidents): This crime can be simply explained as follows – the employee of a company takes advantage of his position for his own financial gain, diverting company funds to himself. The means by which the offender accomplishes the embezzlement varies, depending on the business, from store clerks "skimming" the register to "shady" company accountants falsifying corporate records. This category of fraud has experienced quite a decline in numbers since 1997, when 25 cases were reported. In 2002, a mere five incidents took place, two of which resulted in arrests, including a recurring scenario where two men from Cambridge were impersonating police officers and pulling motorists over in East Cambridge. Once the two suspects pulled their targets over to the side of the road, one man would go to the driver's window, and ask for money as a bribe in exchange for not receiving a citation. Three different victims positively identified the two men who were later apprehended. The other arrest this past year occurred at a clothing store in the Galleria when an employee signed a written confession stating that he stole the deposit bag. Two of the remaining incidents involved known suspects who are pending investigation for offenses at various retail locations.

BAD CHECKS (36 incidents): This scenario is pretty clear-cut: someone writes a check on a closed account or insufficient funds. There were thirty six reports of bad checks in 2002, three of which resulted in arrests.

SCAMS AND CONFIDENCE GAMES (37 incidents): The worst breed of fraud offenders employ "flim-flams" or "con games," which exploit their victims' good will, gullibility, or greed, and bill them for thousands of dollars. We are warned from childhood to beware of offers that are "too good to be true," but our defenses are often overcome by the belief that an offer is "too good to pass up." Three of the major types of scams are listed below.

- ***"The Big Carrot":*** Eight swindles of this type occurred in 2002, six of which occurred in pairs, and all of them probably involved the same suspect or group of suspects. The *modus operandi* was virtually identical from incident to incident: the suspect phoned his victim, claiming to work for an electronic store and had excess merchandise he could sell the victim at a "too good to refuse" price. The two would arrange to meet and exchange the money for the merchandise, but the merchandise never appeared. The victim was usually given a phony receipt and told to wait by the receiving area to pick up the merchandise. The suspect was never seen again. Each victim of this crime was taken for hundreds or thousands of dollars in cash.

- ***The Utility Impostor:*** During these typical scams, the con-artists visit their victims at home, impersonating employees of the electric company, gas company, or water department. While one perpetrator distracts the victim, the other roams the house and collects valuables; he looks primarily for cash, purses, jewelry, or other items that the owner might not notice missing right away. Both incidents this year involved one male suspect who claimed to be from Cambridge/Boston Fire Prevention Corp. and was sent to perform an inspection. During these incidents, property was not stolen, but rather money was swindled out of the victims in exchange for the inspection and for the replacement of fire extinguishers that never showed up. During the first incident, the victim gave up $100 and the second lost over $500.

- ***The Charity Impostor:*** The six incidents this year involved an impostor who poses as a charity worker, collecting cash, which then simply goes into the con man's pocket. The charity impostor may conduct his business door-to-door, or he may stand in the street. The later example was the case in Harvard Square during late August when a homeless man was collecting money for an AIDS charity walk. Once arrested, almost $600 was found on him and over 40 signatures of individualsshowing their support were on a roster. Another incident transpired a month later in Inman Square when two male suspects approached the victim, and convinced him to donate $10,000 in cash to the suspects' father who was in the hospital. One of the men and the victim went to the bank and took money out of the victim's account, which the teller put in a black pouch. The suspects and the victim were supposed to meet later in the day to exchange the money and when the men never showed up, the victim discovered that the bags were switched, and the men got away, while the victim was left with a bank pouch containing newspaper.

- ***"The Pigeon Drop":*** One of the oldest scams in the proverbial book, the pigeon drop is the tool of a fast-talking group of con-artists who prey on the greed and naiveté of their victims. Pigeon drop artists swindled nine Cantabrigians in 2002, one of which resulted in the loss of $13,000. There are several variations of the pigeon drop. In general, the victim is approached on the street by one or two perpetrators and told a story about finding a large sum of money or a winning lottery ticket. The victim is offered a share of the money if they are willing to give the perpetrators a deposit (the swindlers often request money to show the victim's "good faith"). The perpetrators tell a variety of stories about the money and how the victim will

get his or her share. After the victim puts up his or her portion of the cash, the hustlers secretly exchange it for worthless paper or steal it outright. In one version of this scam that happened in 2002, the victim received a phone call from an unknown person calling from Canada, claiming that the victim had won $150,000. In order to get the prize money, the culprit stated that the victim needed to wire $13,000 to Canada and not surprisingly, the victim has yet to receive his winnings. Two similar incidents took place in May when a set of victims received separate phone calls from a man claiming he was from Publisher's Clearing House and that the caller on the other end had won a prize of $100,000 during one call and $1 million in another. In order for the victims to receive their cash, the suspect stated that $4,000 to $6,000 was needed first for taxes and that they should tell no one.

IDENTITY THEFT (115 incidents): Identity theft is a crime in which an imposter obtains key pieces of personal information, such as Social Security or driver's license numbers, in order to impersonate someone else. The information can be used to obtain credit, merchandise, and services in the name of the victim, or to provide the thief with false credentials. In addition to running up debt, an imposter might provide false identification to police, creating a criminal record or leaving outstanding arrest warrants for the person whose identity has been stolen.

- The *New York Newsday* reported in an article dated January 22, 2003, that up to 700,000 people in the United States may be victimized by identity bandits each year, according to the Justice Department. It costs the average victim more than $1,000 in expenses to cope with the damage to their accounts and reputations, the FTC has said. Privacy advocates advise consumers to protect themselves from identity theft by checking their credit reports twice a year, shredding personal documents before throwing them away and cleansing wallets of old receipts and printed Social Security numbers. The number of identity theft complaints rose from about 86,000 in 2001 to about 162,000 last year, the FTC said. Of last year's incidents, 42 percent involved credit card fraud. Other major categories involved fraudulent bank and cell phone accounts. About half of all other types of fraud complaints last year had some connection to the Internet, the FTC said. They involved online transactions, Web site advertising or promotions sent as e-mail spam. The number of complaints about identity theft shot up in 2001 after the FTC began promoting a dedicated Web site and toll-free phone number for victims. In November, federal authorities broke up what they called the biggest identity theft case in U.S. history and charged three men with stealing credit information for 30,000 people. Prosecutors said the scheme began with passwords and records stolen from a software company.

- The District of Columbia had the highest rate of identity theft in 2002 with 123 victims for every 100,000 people. California and Arizona followed with 91 and 88 victims per 100,000 people, respectively.

Preventing Fraud

- Banks are swiftly replacing standard ATM Cards with "Check Cards"—credit cards that deduct directly from your checking account. These check cards, while convenient, present a security problem. Thieves no longer need your Personal Identification Number (PIN) to use the card; if a thief uses it like a credit card, he can drain your entire account by just forging your signature on credit card slips. If your ATM Card has a credit card logo (such as Visa or MasterCard) on it, it can be used like a credit card. If you do not want this feature, notify your bank and have them send you an ATM-only card.
- Keep your credit card numbers, and the telephone numbers of your credit card companies, at home and work. If your cards are stolen, call these numbers immediately and report the theft.
- Try to avoid carrying more credit cards than you need at one time.
- Never write your ATM card PIN number on the card or on a slip of paper in your wallet or purse.
- Protect your cards against theft in the first place; see the prevention tips under the "Larceny" section.
- Merchants should implement and enforce a policy of requiring a photographic identification when using a check or credit card.

Learn to recognize potential fraud scenarios. Any of the following activities almost certainly involves a scam:

- Someone approaches you on the street claiming to have found money.
- Any circumstance in which you have to pay money in order to get money.
- Someone comes to your door, without notification, claiming to work for the gas company, electric company, water company, or cable company. Always ask for official identification and call the utility company to make sure the identification is valid. Do not let "utility impostors" into your home.
- You receive an unsolicited telephone call from someone offering a great deal on some piece of merchandise.
- You're notified in the mail that you've won a prize, but you have to pay money in order to claim it.